

訂正有り

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平2-187888

⑮ Int. Cl.³

識別記号

庁内整理番号

⑬ 公開 平成2年(1990)7月24日

G 06 K 17/00
G 09 C 1/00S 6711-5B
7368-5B

審査請求 未請求 請求項の数 4 (全16頁)

⑭ 発明の名称 認証方式

⑯ 特 願 平1-8010

⑰ 出 願 平1(1989)1月17日

⑱ 発 明 者 飯 島 康 雄 神奈川県川崎市幸区柳町70番地 株式会社東芝柳町工場内
 ⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地
 ⑳ 代 理 人 弁 理 士 鈴 江 武 彦 外3名

明 細 書

1. 発明の名称

認証方式

2. 特許請求の範囲

(1) 第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、

第2の電子装置から第1の電子装置に対し第1のデータおよび、その第1のデータを暗号化するためのキーデータを指定する指定データを送信する手段と、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータの中から前記受信した指定データに基づき1つのキーデータを選択し、この選択したキーデータを使用して前記受信した第1のデータを暗号化する手段と、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうちの一部のデータを第2の電子装置に送信する手段と

を具備したことを特徴とする認証方式。

(2) 第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、

第2の電子装置から第1の電子装置に対し第1のデータおよび、その第1のデータを暗号化するためのキーデータおよび暗号化アルゴリズムを指定する指定データを送信する手段と、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータおよび少なくとも1つの暗号化アルゴリズムの中から前記受信した指定データに基づき1つのキーデータおよび1つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化する手段と、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうちの一部のデータを第2の電子装置に送信する手段と

を具備したことを特徴とする認証方式。

(3) 第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、

第2の電子装置から第1の電子装置に対し第1のデータおよび、その都度内容の異なる第2のデータを送信する手段と、

第1の電子装置において、前記第1のデータおよび第2のデータを受信すると、その受信した第2のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化する手段と、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する手段と

を具備したことを特徴とする認証方式。

(4) 第1の電子装置は、少なくとも1つのメモリ部と、このメモリ部に受信した第1のデータを記憶する手段を更に具備したことを特徴とする請求項1ないし3記載の認証方式。

3. 発明の詳細な説明

[発明の目的]

(産業上の利用分野)

本発明は、たとえばICカード内のメモリ部

装置では、その暗号化データおよび書き込みデータをそれぞれセンタに送り、センタで、これらの各データにより書き込みデータの正当性を確認する認証方式が考えられている。

(発明が解決しようとする課題)

しかし、このような認証方式では、ICカードが多目的利用されるにつれ、複数のアプリケーションで使用されることになった場合、正当性を確認するための各アプリケーションが保管している確認用のキーデータを異ならせる方が、各アプリケーション間のセキュリティを確保するためには有効である。

そこで、本発明は、たとえば複数のアプリケーションでICカードが使用されることになって、各アプリケーションで使用する正当性確認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる認証方式を提供することを目的とする。

また、上記した認証方式では、書き込みデータ、

に対しデータを寄込む際、その書き込みデータの正当性を確認する認証方式に関する。

(従来の技術)

近年、新たな携帯可能なデータ記憶媒体として、消去可能な不揮発性メモリおよび、これらを制御するCPUなどの制御素子を有するICチップを内蔵した、いわゆるICカードが注目されている。

従来、このようなICカードを利用したICカードシステム(たとえばショッピングシステムやクレジットシステムなど)においては、ICカード(実際はICカード内のメモリ部)へのデータ書き込み処理、特に取引データを寄込む際、センタ(ホストコンピュータ)に送られる取引データの正当性がセンタ側で確認できなかった。

このため、端末装置からデータを寄込む命令をICカードが受信すると、ICカード内でキーデータおよび暗号化アルゴリズムを使用して書き込みデータを暗号化し、その暗号化データのうちのデータを端末装置に送り、これを受信した端末

キーデータおよび暗号化アルゴリズムが同一であれば、ICカードから出力される暗号化データも同一となってしまい、本来の取引データの正当性確認が困難となるという問題があった。

そこで、本発明は、同一の書き込みデータ、キーデータおよび暗号化アルゴリズムであっても、書き込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる認証方式を提供することを目的とする。

[発明の構成]

(課題を解決するための手段)

本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、第2の電子装置から第1の電子装置に対し第1のデータおよび、その第1のデータを暗号化するためのキーデータを指定する指定データを送信する手段と、第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータの中から前記受信した指定データに基づ

き1つのキーデータを選択し、この選択したキーデータを使用して前記受信した第1のデータを暗号化する手段と、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する手段とを具備している。

また、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、第2の電子装置から第1の電子装置に対し第1のデータおよび、その第1のデータを暗号化するためのキーデータおよび暗号化アルゴリズムを指定する指定データを送信する手段と、第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータおよび少なくとも1つの暗号化アルゴリズムの中から前記受信した指定データに基づき1つのキーデータおよび1つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化する手段

と、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する手段とを具備している。

さらに、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、第2の電子装置から第1の電子装置に対し第1のデータおよび、その都度内容の異なる第2のデータを送信する手段と、第1の電子装置において、前記第1のデータおよび第2のデータを受信すると、その受信した第2のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化する手段と、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する手段とを具備している。

(作用)

本発明は、ICカード(第1の電子装置)の内部に保有している複数のキーデータのうち1つ

のキーデータを端末装置(第2の電子装置)から指定し、この指定したキーデータを用いて書き込みデータを暗号化することにより、たとえば複数のアプリケーションでICカードが使用されることになっても、各アプリケーションで使用する正当性確認用のキーデータを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

また、本発明は、ICカード(第1の電子装置)の内部に保有している複数のキーデータおよび複数の暗号化アルゴリズムのうち1つのキーデータおよび1つの暗号化アルゴリズムを端末装置(第2の電子装置)から指定し、この指定したキーデータおよび暗号化アルゴリズムを用いて書き込みデータを暗号化することにより、たとえば複数のアプリケーションでICカードが使用されることになっても、各アプリケーションで使用する正当性確認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

さらに、本発明は、端末装置(第2の電子装置)からICカード(第1の電子装置)に送信された、その都度内容の異なるデータをパラメータとして書き込みデータを暗号化することにより、同一の書き込みデータ、キーデータおよび暗号化アルゴリズムであっても、書き込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる。

(実施例)

以下、本発明の一実施例について図面を参照して説明する。

第8図は、本発明に係るICカード(第1の電子装置)と、その上位装置である端末装置(第2の電子装置)と、その上位装置であるセンタ(ホストコンピュータ)とのシステム構成図である。

ICカード(第1の電子装置)10は、各種データを記憶するためのメモリ部11、乱数データを発生する乱数発生部12、データの暗号化を行なう暗号化部13、後述する端末装置20と通信するためのコンタクト部14、およびこれらを制

御するCPUなどの制御素子15などから構成されており、これらのうちメモリ部11、乱数発生部12、暗号化部13および制御素子15は、たとえば1つのICチップ（あるいは複数のICチップ）で構成されてICカード本体内に埋設されている。

メモリ部11は、たとえばEEPROMなどの不揮発性メモリによって構成されており、第2図に示すように、エリア定義テーブル（領域）16とデータファイル（領域）17とに大きく分割されている。そして、データファイル17内は、図示するように複数のエリア18、…に分割定義されるもので、これら各エリア18…はエリア定義テーブル16内のエリア定義情報19によってそれぞれ定義される。

ここに、エリア定義情報19は、たとえばエリアを指定する識別情報としてのエリア番号（AID）、エリアが割当てられているメモリ上の先頭アドレス情報、エリアの容量を規定するサイズ情報および属性情報を対応付けたデータ列で

キーデータリストはキーデータ番号とキーデータとを対応付けたリストであり、KIDリストはキーデータを指定するキーデータ番号のみがリスト化されたものである。一方、ICカード10は、独自にキーデータリストを有しており、これはカード発行時などで内部のメモリ部11に登録（記憶）される。

さて、まずステップ1～ステップ8によって、ICカード10と端末装置20との間で行なわれる相互認証のプロセスを説明する。まず、ステップ1において、端末装置20は、乱数発生部22によって乱数データR1を生成し、認証準備コマンドEXCHによって、これをICカード10に送信する。このとき、端末装置20がICカード10を認証するために使用するキーデータのキーデータ番号（KID-M）、および端末装置20がサポートしている暗号化アルゴリズム（ALG）の指定データをも合わせて送信する。

次に、ステップ2において、ICカード10は、認証準備コマンドEXCHを受信すると、乱数発

生部22によって乱数データR2を生成し、それを認証準備コマンドEXCHに対するレスポンスexchとして端末装置20に送信する。このとき、ICカード10は、端末装置20を認証するために使用するキーデータのキーデータ番号（KID-N）を自身のもつキーリストより見付けだし、かつ指定された暗号化アルゴリズム（ALG）を自身がサポートしているかを判断し、これをalgとして乱数データR2と合わせて端末装置20に送信する。

もしこのとき、端末装置20から指定されたキーデータ番号（KID-M）がキーリストに存在しなかったり、あるいはICカード10が端末装置20を認証するために使用するキーデータ番号（KID-N）がキーリストに存在しなかったり、あるいは指定された暗号化アルゴリズムをサポートしていなかった場合には、その旨を端末装置20に通知する。

次に、このような構成において、本発明に係る認証方式を第1図を用いて詳細に説明する。なお、端末装置20のメモリ部21には、図示するようなキーデータリストおよびキーデータ番号（KID）リストが格納されているものとする。

次に、ステップ3において、端末装置20は、ICカード10から指定された暗号化キーデータ

のキーデータ番号 (K I D - N) を自己が所有するキーリストから探し出し、対応するキーデータ (N N N N N) を取出す。そして、暗号化部 23 によって、暗号化アルゴリズム A L G (= a l g) を使用してキーデータ (N N N N N) により I C カード 10 からの乱数データ R 2 を暗号化し、その結果、すなわち暗号化データ C 2 を認証コマンド A U T H によって I C カード 10 に送信する。なお、図中、E は暗号化を実現する機能ボックスを示す。

次に、ステップ 4 において、I C カード 10 が認証コマンド A U T H を受信すると、I C カード 10 は、先に送信した暗号化キーデータのキーデータ番号 (K I D - N) を自己が所有するキーリストより探し出し、対応するキーデータ (N N N N N) を取出す。そして、暗号化部 13 によって、認証準備コマンド E X C H で指定された暗号化アルゴリズム (A L G) を使用してキーデータ (N N N N N) により乱数データ R 2 を暗号化し、暗号化データ C 2 X を得る。

(M M M M M) を取出す。そして、暗号化部 23 によって、暗号化アルゴリズム (A L G) を使用してキーデータ (M M M M M) により端末装置 20 からの乱数データ R 1 を暗号化し、暗号化データ C 1 X を得る。

次に、ステップ 8 において、端末装置 20 は、レスポンス a u t h によって受信した暗号化データ C 1 とステップ 7 で生成した暗号化データ C 1 X とを比較し、この比較結果とレスポンス a u t h により受信したステップ 5 による I C カード 10 での比較結果とにより、以降のシステム処理の決定を行なう。

次に、ステップ 9 ～ ステップ 23 によって、端末装置 20 から I C カード 10 に対しデータを書込むとともに、書込み処理の正当性を確認するプロセスを説明する。まず、ステップ 9 において、端末装置 20 は、書込みコマンド W R I T E によりデータを書込む要求を I C カード 10 に送信する。このとき、端末装置 20 は、I C カード 10 内のメモリ部 11 に対する書込み対象エリアのエ

次に、ステップ 5 において、I C カード 10 は、先に受信した認証コマンド A U T H 中の暗号化データ C 2 とステップ 4 で生成した暗号化データ C 2 X とを比較し、その比較結果 Y / N を得る。

次に、ステップ 6 において、I C カード 10 は、認証準備コマンド E X C H で端末装置 20 から指定された暗号化キーデータのキーデータ番号 (K I D - M) に対応するキーデータ (M M M M M) を取出す。次に、暗号化部 13 によって、暗号化アルゴリズム (A L G) を使用してキーデータ (M M M M M) により乱数データ R 1 を暗号化し、暗号化データ C 1 を得る。そして、この暗号化データ C 1 とステップ 5 による比較結果 Y / N を、認証コマンド A U T H に対するレスポンス a u t h として端末装置 20 に送信する。

次に、ステップ 7 において、端末装置 20 がレスポンス a u t h を受信すると、端末装置 20 は、先に送信した暗号化キーデータのキーデータ番号 (K I D - M) に対応するキーデータ

リア番号 (A I D - A)、書込みデータのバイト数 (L - 1)、および書込みデータ (M 1) のうち I C カード 10 が入力データとして受信し得るバイト数に分割した最初の分割データ (M 1 - 1) を I C カード 10 に送信する。

次に、ステップ 10 において、I C カード 10 は、書込みコマンド W R I T E によって受信したエリア番号 (A I D - A) が付されたエリアを第 2 図のエリア定義テーブル 16 から見付ける。もし見付からなければ、エリア番号未定義を意味するステータスを書込みコマンド W R I T E に対するレスポンス w r i t e によって端末装置 20 に送信する。もし見付かれれば、先に認証準備コマンド E X C H、または後述する暗号化準備コマンド S R N D が正常終了されているかをチェックする。

このチェックの結果、もし正常終了されていないければ、実行条件不備ステータスをレスポンス w r i t e によって端末装置 20 に送信する。上記チェックの結果、正常終了されていければ、I C カード 10 は、先の認証準備コマンド

EXCHによって通知された乱数データR1とICカード10の内部で所有するカード固有値とにより初期データR1'を生成する。

次に、ステップ11において、ICカード10は、先に認証準備コマンドEXCHで指定された暗号化アルゴリズム(ALG)を使用して、初期データR1'および先に認証準備コマンドEXCHによって通知されたキーデータ番号(KID-M)に対応するキーデータ(MMMMM)により書込みデータ(M1-1)を暗号化し、暗号化データ(C1-1)を得る。次に、アクセス対象となっているエリア番号(AID-A)のエリアの属性情報を参照することにより、メモリ部11への書込みデータを入力データ(M1-1)にするか暗号化データ(C1-1)にするかを決定し、書込み処理を行なう。そして、端末装置20に対し次の書込みデータを要求するためのレスポンス`nb`を送信する。

次に、レスポンス`nb`を受信すると、端末装置20は、ステップ12において、次の書込み

データ(M1-2)をICカード10に送信する。次に、ステップ13において、次の書込みデータ(M1-2)を受信すると、ICカード10は、再び暗号化アルゴリズム(ALG)を使用して、先に生成した暗号化データ(C1-1)の最終の8バイトデータおよびキーデータ番号(KID-M)に対応するキーデータ(MMMMM)により書込みデータ(M1-2)を暗号化し、暗号化データ(C1-2)を得る。次に、ステップ11と同様に、メモリ部11への書込みデータを入力データ(M1-2)にするか暗号化データ(C1-2)にするかを決定し、選択的にエリアへの書込み処理を行なう。そして、端末装置20に対し次の書込みデータを要求するためのレスポンス`nb`を送信する。

以下、ステップ12、13と同様の処理動作を繰返し行なう。

さて、ステップ14において、端末装置20が分割データの最終データ(M1-n)をICカード10に送信すると、ステップ15において、

ICカード10は同様の書込み処理を行なう。そして、最終的に生成された暗号化データ(C1-n)のうち最終8バイトを確認情報(AC1)とし、書込みコマンドWRITEに対するレスポンス`write`によって端末装置20に送信する。

すなわち、上記処理においては、あらかじめ相互認証手順で端末装置20がICカード10を認証するために、ICカード10に対して指定したキーデータ(MMMMM)、暗号化アルゴリズム(ALG)および乱数データ(R1)を使用して、書込みデータM1に対する確認情報(AC1)が得られている。

次に、上記とは異なるキーデータ、暗号化アルゴリズムおよび乱数データにより確認情報を得るプロセスをステップ16～ステップ20によって説明する。まず、ステップ16において、端末装置20は、乱数発生部22によって新規の乱数データR3を生成し、暗号化準備コマンドSRNDによって、これをICカード10に送信する。このとき、ICカード10が確認情報を生成するの

に使用するキーデータのキーデータ番号(KID-A)、および暗号化アルゴリズム(ALG)を合わせて送信する。

次に、ステップ17において、ICカード10は、暗号化準備コマンドSRNDを受信すると、キーデータ番号(KID-A)を自身が所有するキーリストから見付けだし、対応するキーデータ(AAAAA)を得て、レスポンス`s_rnd`を端末装置20に送信する。

次に、ステップ18において、端末装置20は、書込みコマンドWRITEによりデータを書込む要求をICカード10に送信する。このとき、端末装置20は、ICカード10内のメモリ部11に対する書込み対象エリアのエリア番号(AID-B)、書込みデータのバイト数(L-2)、および書込みデータ(M2)を送信する。なお、本ステップ18では、書込みデータ(M2)のバイト数は、ICカード10が入力データとして受信し得るバイト数である。

次に、ステップ19において、ICカード10

は、ステップ10と同様にしてエリア番号(AID-B)が付されたエリアを第2図におけるエリア定義テーブル16から見付ける。そして、次にICカード10として、先に暗号化準備コマンドSRND(または認証準備コマンドEXCH)が正常終了されているか否かをチェックする。もし、正常終了されているとすると、ICカード10は、暗号化準備コマンドSRNDによって通知された乱数データR3とICカード10の内部で所有するカード固有値とにより初期データR3'を生成する。

次に、ステップ20において、ICカード10は、先に暗号化準備コマンドSRNDで指定された暗号化アルゴリズム(ALG')を使用して、初期データR3'および先に暗号化準備コマンドSRNDにより通知されたキーデータ番号(KID-A)に対応するキーデータ(AAAAA)により書込みデータ(M2)を暗号化し、暗号化データC2を得る。次に、アクセス対象となっているエリア番号(AID-B)の

エリアの属性情報を参照することにより、メモリ部11への書込みデータを入力データ(M2)にするか暗号化データ(C2)にするかを決定し、書込み処理を行なう。そして、端末装置20に対し、暗号化データ(C2)のうち最終8バイトのデータを確認情報(AC2)として、書込みコマンドWRITEに対するレスポンスwriteによって送信する。

なお、ICカード10は、第2図のエリア定義テーブル16内の先頭アドレス情報およびサイズ情報によりメモリ部11内の物理的位置を確認する。先頭アドレス情報は対応するエリアの先頭アドレス値であり、サイズ情報は先頭アドレス値からのエリアの容量を規定している。また、属性情報は1バイトで構成され、そのMSBが「0」であれば暗号化データ書込みエリアであり、「1」であれば入力データ書込みエリアであることを示す。

次に、ステップ21において、端末装置20は、ICカード10へのデータ書込みを終了すると、

書込みデータ(M1, M2)に対応する乱数データ(R1, R3)、キーデータ番号(KID-M, KID-A)、確認情報(AC1, AC2)、および使用アルゴリズム指定値(ALG, ALG')により、データ書込み処理リストを作成する。なお、このときカード固有値もリストに対応付けておく。そして、この作成したリストをセンタ30へ送信する。

次に、ステップ22において、センタ30は、端末装置20からのリストを受信すると、そのリストから書込みデータ(M1)を取出し、対応するキーデータ番号(KID-M)により、キーデータ(MMMMM)を自身が所有するキーリストから見付けだし、かつ自身が所有する取引リストで対応付けられている乱数データ(R1)および暗号化アルゴリズム(ALG)により確認情報(AC1X)を生成する。

そして、ステップ23において、リストで対応付けられた確認情報(AC1)とステップ22で生成した確認情報(AC1X)とを比較し、両者

が一致していればセンタ30は書込みデータ(M1)に対する書込み処理の正当性を確認する。

書込みデータ(M2)以降についても、ステップ22, 23と同様な処理により正当性を確認する。

次に、ICカード10としての動作を第7図を用いて説明する。まず、制御素子15は、端末装置20からの制御信号によって電気的活性化を経た後、アンサー・ツー・リセットと称する初期応答データを端末装置20へ出力する(S1)。そして、制御素子15は、認証準備コマンド完了フラグおよび暗号化準備コマンド完了フラグをオフし(S2)、命令データ待ち状態に移る。

この状態で、命令データを受信すると(S3)、制御素子15は、まず、この命令データが第3図に示す認証準備コマンドEXCHであるか否かを判断し(S4)、もしそうでないと判断すると次のフローに移る。

ステップS4において、認証準備コマンドEXCHであると判断すると、制御素子15は、

認証準備コマンド中のキーデータ番号 (KID) フィールドの内容をピックアップし、メモリ部 11 内に登録されているキーリストから同一のキーデータ番号を見付ける (S5)。

そして、もしキーデータ番号が見付からなければ (S6)、制御素子 15 は、キーデータ指定エラーステータスを出力し (S7)、命令データ待ち状態に戻る。もし、キーデータ番号が見付かれれば (S6)、制御素子 15 は、対応するキーデータを内部 RAM 上の第 1 キーバッファにセーブする (S8)。

次に、制御素子 15 は、認証準備コマンド中の暗号化アルゴリズム指定データ (ALG) フィールドを参照することにより、メモリ上に登録されている暗号化アルゴリズムであるか否かをチェックする (S9)。このチェックの結果、指定された暗号化アルゴリズムが存在しない場合 (S10)、制御素子 15 は、指定アルゴリズムエラーステータスを出力し (S11)、命令データ待ち状態に戻る。上記チェックの結果、指定

された暗号化アルゴリズムが存在する場合 (S10)、制御素子 15 は、その暗号化アルゴリズムの番号をセーブしておく (S12)。

次に、制御素子 15 は、認証準備コマンド中の乱数データ (R1) を内部 RAM 上の第 1 乱数バッファにセーブし (S13)、その後、先のキーリストから IC カード認証用キーデータのキーデータ番号 (KID') を見付ける (S14)。

そして、もしキーデータ番号が見付からなければ (S15)、制御素子 15 は、キーデータ未登録エラーステータスを出力し (S16)、命令データ待ち状態に戻る。もし、キーデータ番号が見付かれれば (S15)、制御素子 15 は、対応するキーデータを内部 RAM 上の第 2 キーバッファにセーブする (S17)。

次に、制御素子 15 は、乱数発生部 12 によって乱数データ R2 を生成し、内部 RAM 上の第 2 乱数バッファにセーブする (S18)。そして、制御素子 15 は、認証準備コマンド完了フラグをオンし (S19)、かつ、生成した乱数データ

R2 を先のキーデータ番号 (KID') および認証準備コマンド中の暗号化アルゴリズム指定データ (ALG) フィールドの内容とともに、認証準備コマンド EXCH に対するレスポンス exch として端末装置 20 に出力し (S20)、命令データ待ち状態に戻る。

ステップ S4 において、認証準備コマンド EXCH でないと判断すると、制御素子 15 は、第 4 図に示す認証コマンド AUTH であるか否かを判断し (S21)、もしそうでないと判断すると次のフローへ移る。

ステップ 21 において、認証コマンド AUTH であると判断すると、制御素子 15 は、認証準備コマンド完了フラグがオンされているか否かを判断し (S22)、もしオフであれば実行条件不備エラーステータスを出力し (S23)、命令データ待ち状態に戻る。

ステップ 22 において、認証準備コマンド完了フラグがオンであれば、制御素子 15 は、暗号化部 13 により、第 2 キーバッファの内容を暗号化

のキーデータとして第 2 乱数バッファの内容を暗号化する (S24)。このときの暗号化アルゴリズムは、セーブされた暗号化アルゴリズム番号に対応する暗号化アルゴリズムを使用する。

そして、制御素子 15 は、上記暗号化の結果と認証コマンド AUTH で送られた入力データとを比較し (S25)、その比較結果に応じて一致フラグをオンまたはオフする (S26～S28)。

次に、制御素子 15 は、暗号化部 13 により、第 1 キーバッファの内容を暗号化のキーデータとして第 1 乱数バッファの内容を暗号化する (S29)。このときの暗号化アルゴリズムも上記同様のものを使用する。そして、制御素子 15 は、この暗号化の結果を先の一致フラグの内容とともに、認証コマンド AUTH に対するレスポンス auth として端末装置 20 に出力し (S30)、命令データ待ち状態に戻る。

ステップ S21 において、認証コマンド AUTH でないと判断すると、制御素子 15 は、第 5 図に示す暗号化準備コマンド SRND である

か否かを判断し(S31)、もしそうでないと判断すると次のフローへ移る。

ステップ31において、暗号化準備コマンドSRNDであると判断すると、制御素子15は、暗号化準備コマンド中のキーデータ番号(KID)フィールドの内容をピックアップし、メモリ部11内に登録されているキーリストから同一のキーデータ番号を見付ける(S32)。

そして、もしキーデータ番号が見付からなければ(S33)、制御素子15は、キーデータ指定エラーステータスを出力し(S34)、命令データ待ち状態に戻る。もし、キーデータ番号が見付かれれば(S33)、制御素子15は、対応するキーデータを内部RAM上の第1キーバッファにセーブする(S35)。

次に、制御素子15は、暗号化準備コマンド中の暗号化アルゴリズム指定データ(ALG)フィールドを参照することにより、メモリ上に登録されている暗号化アルゴリズムであるか否かをチェックする(S36)。このチェックの結果、指定

された暗号化アルゴリズムが存在しない場合(S37)、制御素子15は、指定アルゴリズムエラーステータスを出力し(S38)、命令データ待ち状態に戻る。上記チェックの結果、指定された暗号化アルゴリズムが存在する場合(S37)、制御素子15は、その暗号化アルゴリズムの番号をセーブしておく(S39)。

次に、制御素子15は、暗号化準備コマンド中の乱数データ(R3)を内部RAM上の第1乱数バッファにセーブし(S40)、その後、暗号化準備コマンド完了フラグをオンし(S41)、かつ暗号化準備コマンド完了ステータスを端末装置20に出力し(S42)、命令データ待ち状態に戻る。

ステップS31において、暗号化準備コマンドSRNDでないと判断すると、制御素子15は、第6図(a)または(b)に示す書き込みコマンドWRITEであるか否かを判断し(S51)、もしそうでないと判断すると、他のコマンド(たとえばデータの読出しコマンド)であるか否かの判

断を行ない、対応する処理へ移行する。

ステップS51において、書き込みコマンドWRITEであると判断すると、制御素子15は、その書き込みコマンドが第6図(a)の形式か(b)の形式かを判断し(S52)、第6図(a)の書き込みコマンドであれば、認証準備コマンド完了フラグおよび暗号化準備コマンド完了フラグを参照し(S53)、どちらかでもオフとなっていれば(S54)、条件不備ステータスを出力し(S55)、命令データ待ち状態に戻る。もしどちらかのフラグがオンとなっていれば(S54)、制御素子15は、書き込みコマンド中のデータ部の内容を内部RAM上の第2ライトバッファにセーブする(S56)。

ステップS52において、第6図(b)の書き込みコマンドであれば、制御素子15は、内部で保持している書き込みコマンド継続フラグがオン否かを判断する(S57)。もしオフとなっていれば、制御素子15は、要求エラーステータスを出力し(S58)、命令データ待ち状態に戻る。

もしオンとなっていれば、制御素子15は、内部RAM上のデータセーブバッファの内容に書き込みコマンド中のデータ部の内容(入力データ)を付加し、内部RAM上の第2ライトバッファにセーブする(S59)。

そして、制御素子15は、書き込みコマンド中のデータ部の内容(入力データ)のみを内部RAM上の第1ライトバッファにセーブする(S60)。

次に、制御素子15は、第6図(a)または(b)の書き込みコマンドによって送られた入力データに書き込み後続データが存在するか否かをチェックし(S61)、書き込み後続データが存在すれば後続フラグをオンし(S62)、書き込み後続データが存在しなければ後続フラグをオフする(S63)。

次に、制御素子15は、内部RAM上の第2ライトバッファ内のデータのバイト数が例えば「8」の倍数であるか否かをチェックし(S64)、もしそうでなければステップS70に移行する。もしそうでなければ、制御素子15は、後続フラグを

参照してオフとなっていれば(S65)、内部RAM上の第2ライトバッファ内のデータにパディング処理(たとえば「20」ヘッダデータを後ろに付加)し(S66)、「8」の倍数分のデータを生成してステップS70に移行する。

ステップS65において、後続フラグがオンとなっていれば、制御素子15は、「8」の倍数分のデータを残し、残りのデータを内部RAM上のデータセーブバッファに移動する(S67)。すなわち、たとえば第2ライトバッファに18バイトのデータが存在すれば、16バイトのデータのみを残して残りの2バイトはデータセーブバッファに移動する。このとき、内部RAM上の第2ライトバッファ内が空となっていなければ(S68)、ステップS70に移行する。

ステップS68において、内部RAM上の第2ライトバッファ内が空となっていれば(たとえば第2ライトバッファ内に7バイトのデータがあれば、先の処理で第2ライトバッファ内のデータ全てがデータセーブバッファに移動されるため、結

果として第2ライトバッファは空となる)、制御素子15は、今回アクセスしているエリアが書き込み時に暗号化するエリアか否かを判断する(S69)。そして、もしそうでなければステップS71に移行し、もしそうであればステップS79に移行する。

さて、ステップS70において、制御素子15は、暗号化部13により、内部RAM上の第2ライトバッファ内のデータを例えばCBCモードで暗号化する。このとき、継続フラグがオフとなっていれば、内部RAM上の第1乱数バッファの内容にカード固有値を排他的論理和したものを、また継続フラグがオンとなっていれば、前回の書き込みで暗号化したデータの最終8バイトをそれぞれ初期値として、今回のCBCモード暗号化に使用する。また、このときのキーデータは第1キーバッファの内容を使用し、暗号化アルゴリズムは保持されている暗号化アルゴリズム番号により選択的に使用する。そして、この処理が終了するとステップS71に移行する。

ステップS71において、制御素子15は、継続フラグがオンされているか否かを判断し、オンされていればアクセス対象エリアが暗号化を要するエリアか否かを判断する(S72)。もし暗号化を要するエリアでなければ、制御素子15は、内部RAM上の第1ライトバッファの内容に書き込みコマンド中の書き込みデータのバイト数LXを付加して、メモリ部11のアクセス対象エリア内にデータを蓄積する(S73)。また、もし暗号化を要するエリアであれば、制御素子15は、書き込みデータのバイト数LXよりも大なる「8」の倍数で、最少の値をLX'とし、これを第2ライトバッファ内のデータを付加して蓄積する(S74)。

ステップS71において、継続フラグがオンされていれば、制御素子15は、アクセス対象エリアが暗号化を要するエリアか否かを判断する(S75)。もし暗号化を要するエリアでなければ、制御素子15は、内部RAM上の第1ライトバッファの内容を先に蓄積したデータに追加して蓄積する(S76)。また、もし暗号化を要するエ

リアであれば、制御素子15は、内部RAM上の第2ライトバッファの内容を同様に蓄積する(S77)。

さて、データを蓄積した後、制御素子15は、継続フラグがオンされているか否かを判断し(S78)、オンされていれば継続フラグをオンしてレスポンス「nb」を出力し(S79)、命令データ待ち状態に戻る。もし、継続フラグがオフとなっていれば、制御素子15は、内部RAM上の第2ライトバッファの内容の最終8バイトを出力して継続フラグをオフし(S80)、命令データ待ち状態に戻る。

このように、ICカードの内部に保有している複数のキーデータおよび複数の暗号化アルゴリズムのうち1つのキーデータおよび1つの暗号化アルゴリズムを端末装置から指定し、この指定したキーデータおよび暗号化アルゴリズムを用いて書き込みデータを暗号化することにより、複数のアプリケーションでICカードが使用されることになっても、各アプリケーションで使用する正当性確

認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

なお、端末装置20からICカード10に送信される乱数データR1、R3は、その都度内容が同一のデータであってもよいが、その都度内容の異なるデータとすることにより、同一の書き込みデータ、キーデータおよび暗号化アルゴリズムであっても、書き込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる。

この場合、端末装置20内において、たとえば時計回路を設け、この時計回路から発生する時間情報を用いて乱数データR1、R3を生成することにより、容易にその都度内容の異なるデータを得ることができる。

〔発明の効果〕

以上詳述したように本発明の認証方式によれば、たとえば複数のアプリケーションでICカードが使用されることになっても、各アプリケーシ

ョンで使用する正当性確認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

また、本発明の認証方式によれば、同一の書き込みデータ、キーデータおよび暗号化アルゴリズムであっても、書き込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる。

4. 図面の簡単な説明

図は本発明の一実施例を説明するためのもので、第1図はICカードと端末装置との間の相互認証手順および端末装置からICカードへのデータ書き込み手順を示す図、第2図はメモリ部の構成を示す図、第3図は認証準備コマンドのフォーマット例を示す図、第4図は認証コマンドのフォーマット例を示す図、第5図は暗号化準備コマンドのフォーマット例を示す図、第6図は書き込みコマンドのフォーマット例を示す図、第7図はICカードの動作を説明するフローチャート、第8図はIC

カードと端末装置とセンタとのシステム構成図である。

10…ICカード（第1の電子装置）、11…メモリ部、12…乱数発生部、13…暗号化部、14…コンタクト部、15…制御素子、20…端末装置（第2の電子装置）、21…メモリ部、22…乱数発生部、23…暗号化部、26…コンタクト部、27…通信制御部、28…制御部、30…センタ（ホストコンピュータ）。

機能コード	KID	ALG	R1
-------	-----	-----	----

第3図

機能コード	データ列
-------	------

第4図

機能コード	KID	ALG	R3
-------	-----	-----	----

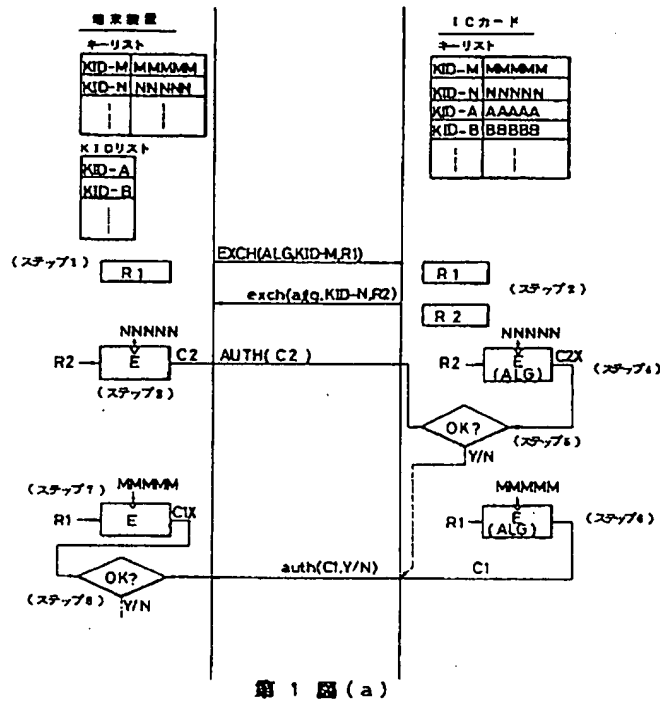
第5図

(a) 機能コード	AID	LX	データ部
-----------	-----	----	------

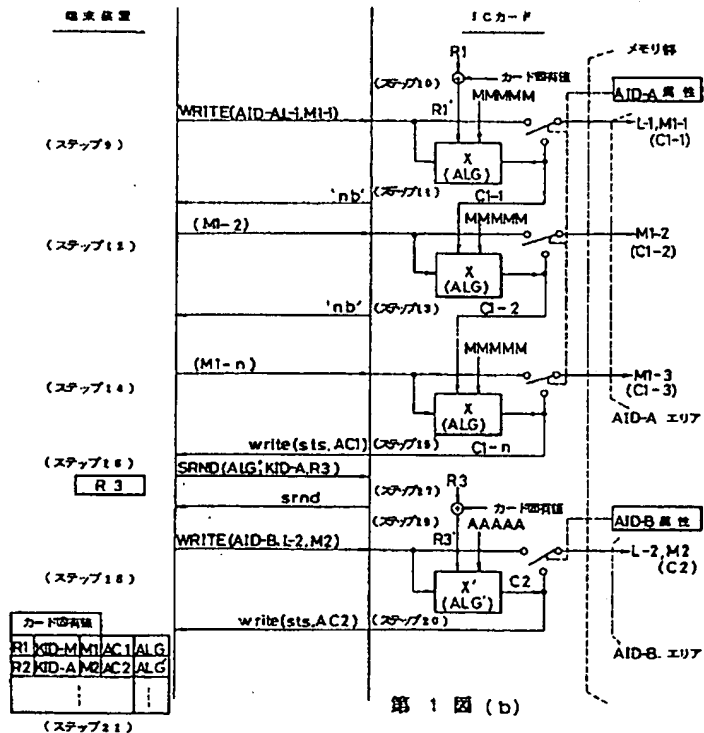
(b) 認証要求機能コード	データ部
---------------	------

第6図

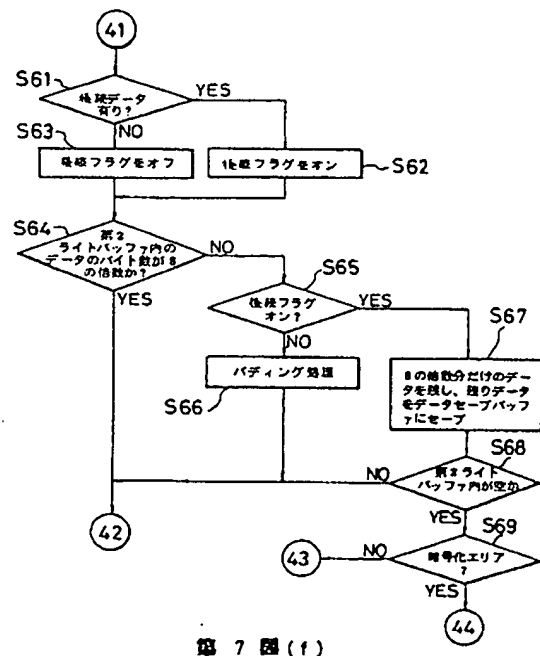
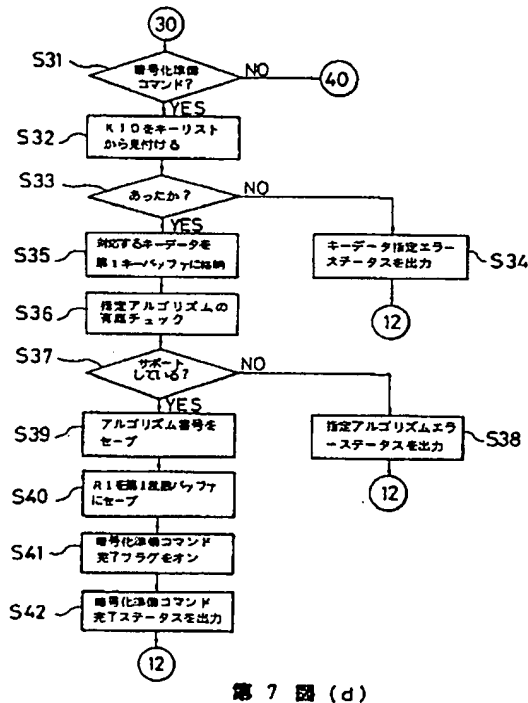
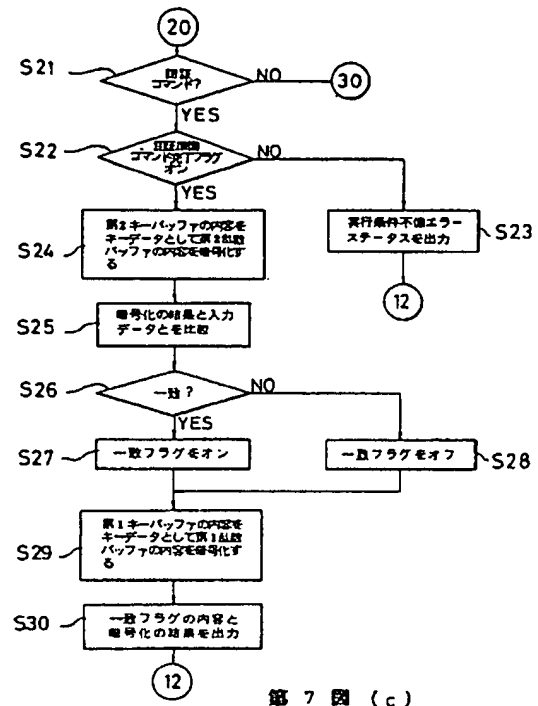
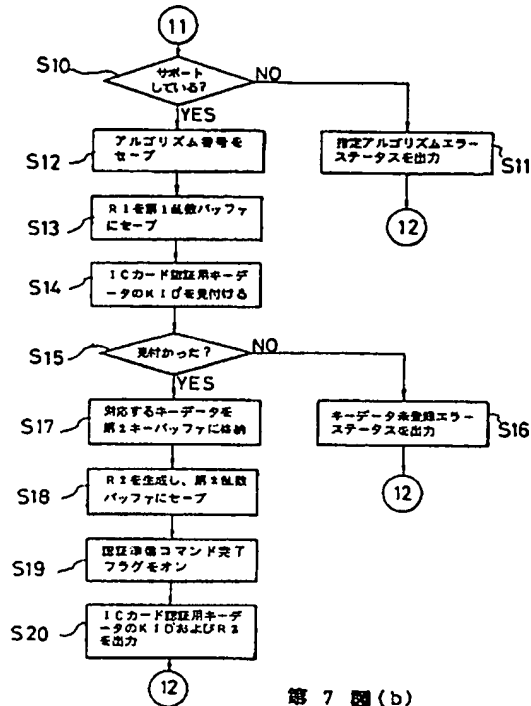
出願人代理人 弁理士 鈴 江 武 彦

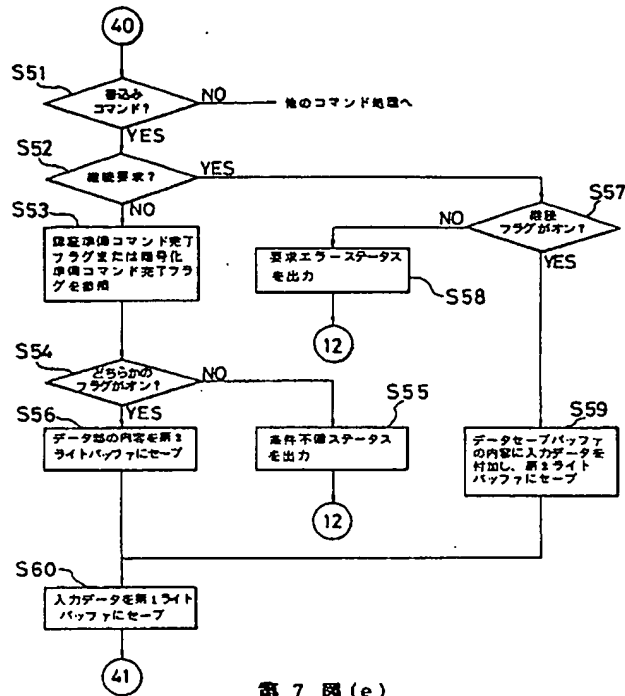


第1図(a)

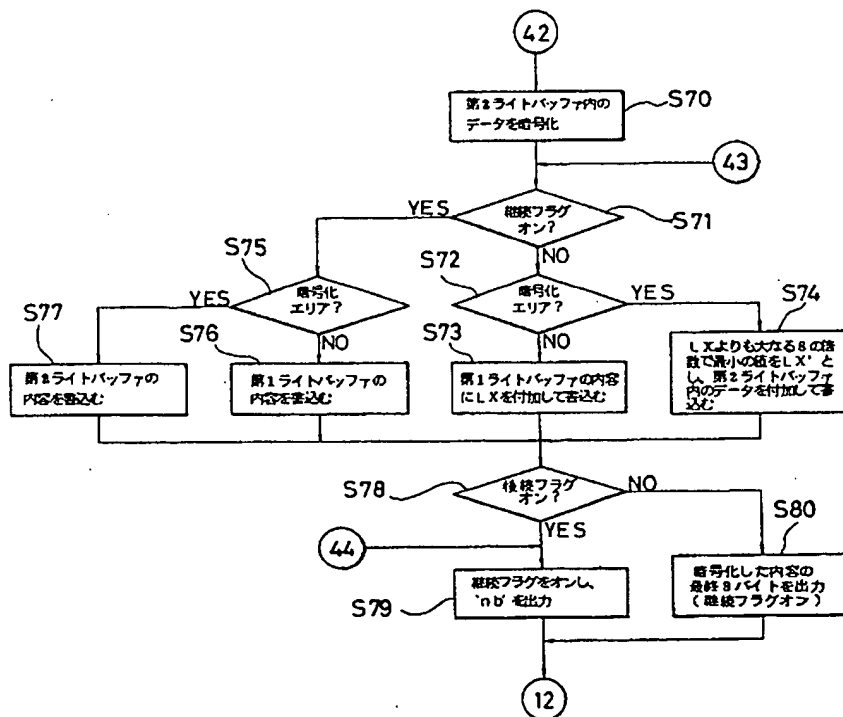


第1図(b)

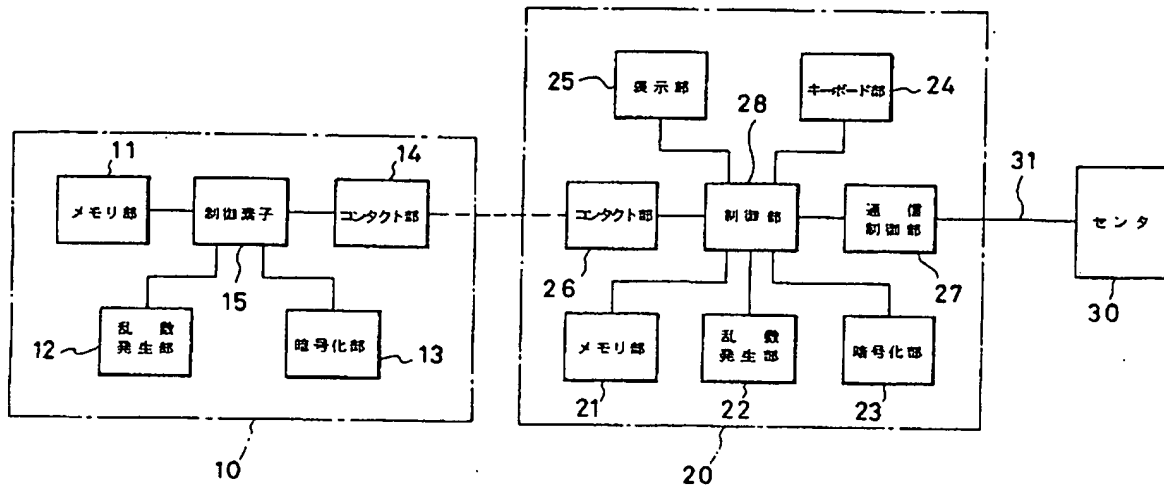




第 7 図 (e)



第 7 図 (g)



第 8 図

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成8年(1996)12月24日

【公開番号】特開平2-187888

【公開日】平成2年(1990)7月24日

【年通号数】公開特許公報2-1879

【出願番号】特願平1-8010

【国際特許分類第6版】

G06K 17/00

G09C 1/00

【F1】

G06K 17/00 S 7623-5B

G09C 1/00 7259-5J

特許 補正 出願 番号

平成 年 月 日

特許庁長官 清川 佑二 殿

1. 事件の表示

特 願 平 1 - 8 0 1 0 号

2. 発明の名称

認 証 方 式

3. 補正をする者

事件との関係 特許出願人

(307) 株式会社 東芝

4. 代理人

東京都千代田区西が岡3丁目7番2号

鈴 屋 内 外 国 特 許 事 務 所 内

〒100 電話03(3502)3181(大代表)

(5847) 非理士 鈴 江 武 彦



5. 自発補正

6. 補正の対象

明 細 書

7. 補正により増加する請求項の数 1



8. 補正の内容

(1) 特許請求の範囲を別紙の通り訂正する。

(2) 明細書の第6頁第12行目ないし第8頁第17行目にわたって「本発明の認証方式は、……具備している。」とあるを下記の通り訂正する。

記

本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータを指定する指定データを送信し、第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータの中から前記受信した指定データに基づき1つのキーデータを選択し、この選択したキーデータを使用して前記受信した第1のデータを暗号化し、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信することを特徴としている。

また、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータ、および、暗号化アルゴリズムを指定する指定データを送信し、第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータおよび少なくとも1つの暗号化アルゴリズムの中から前記受信した指定データに基づき1つのキーデータおよび1つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうちの一部のデータを第2の電子装置に送信することを特徴としている。

また、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、第2の電子装置から第1の電子装置に対し第1のデータ、および、その暗号化データの異なる第

2のデータを送信し、第1の電子装置において、前記第1のデータおよび第2のデータを受信すると、その受信した第2のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信することを特徴としている。

さらに、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子との間で行なわれる認証方式において、第1の電子装置および第2に電子装置のそれぞれにおいて複数のキーデータを記憶しておき、第1の電子装置から第2の電子装置に対してキーデータを指定する第1のキー指定データおよび第1のデータを送信し、第2の電子装置から第1の電子装置に対してキーデータを指定する第2のキー指定データおよび第2のデータを送信し、第2の電子装置では、この第1のキー指定データにより指定されたキーデータを検出して、このキーデータを用いて第1のデータを暗号化して第1の認証データを作成し、第2の電子装置から第1の電子装置に対して第1の認証データを送信し、第1の電子装置において送信した第1のキー指定データに対応するキーデータを検出して、このキーデータを用いて第1のデータを暗号化して第2の認証データを作成し、第1の電子装置において第2の認証データと第2の電子装置から送信されてきた第1の認証データと比較して第2の電子装置の正当性を確認し、第1の電子装置において受信した第2のキー指定データにより指定されたキーデータを検出して、このキーデータを用いて第2のデータを暗号化して第3の認証データを作成し、第2の電子装置の正当性が確認された場合は、第2の認証データと第1の認証データとの比較結果および第1の電子装置において作成した第3の認証データを第2の電子装置へ送信し、第2の電子装置の正当性が確認されなかった場合は、第2の認証データと第1の認証データとの比較結果を第1の電子装置から第2の電子装置に対して送信することを特徴としている。

第1の電子装置において、前記第1のデータおよび第2のデータを受信すると、その受信した第2のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する

ことを特徴とする認証方式。

(4) 第1の電子装置は、少なくとも1つのメモリ部と、このメモリ部に受信した第1のデータを記憶する手段を更に具備したことを特徴とする請求項1ないし3記載の認証方式。

(5) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子との間で行なわれる認証方式において、

第1の電子装置および第2に電子装置のそれぞれにおいて複数のキーデータを記憶しておき、

第1の電子装置から第2の電子装置に対してキーデータを指定する第1のキー指定データおよび第1のデータを送信し、

第2の電子装置から第1の電子装置に対してキーデータを指定する第2のキー指定データおよび第2のデータを送信し、

第2の電子装置では、この第1のキー指定データにより指定されたキーデータを検出して、このキーデータを用いて第1のデータを暗号化して第1の認証データを作成し、

第2の電子装置から第1の電子装置に対して第1の認証データを送信し、

第1の電子装置において送信した第1のキー指定データに対応するキーデータを検出して、このキーデータを用いて第1のデータを暗号化して第2の認証データを作成し、

第1の電子装置において第2の認証データと第2の電子装置から送信されてきた第1の認証データと比較して第2の電子装置の正当性を確認し、

第1の電子装置において受信した第2のキー指定データにより指定されたキーデータを検出して、このキーデータを用いて第2のデータを暗号化して第3の認証データを作成し、

2. 特許請求の範囲

(1) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、

第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータを指定する指定データを送信し、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータの中から前記受信した指定データに基づき1つのキーデータを選択し、この選択したキーデータを使用して前記受信した第1のデータを暗号化し、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する

ことを特徴とする認証方式。

(2) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、

第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータ、および、暗号化アルゴリズムを指定する指定データを送信し、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータおよび少なくとも1つの暗号化アルゴリズムの中から前記受信した指定データに基づき1つのキーデータおよび1つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する

ことを特徴とする認証方式。

(3) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、

第2の電子装置から第1の電子装置に対し第1のデータ、および、その都度内容の異なる第2のデータを送信し、

第2の電子装置の正当性が確認された場合は、第2の認証データと第1の認証データとの比較結果および第1の電子装置において作成した第3の認証データを第2の電子装置へ送信し、

第2の電子装置の正当性が確認されなかった場合は、第2の認証データと第1の認証データとの比較結果を第1の電子装置から第2の電子装置に対して送信する

ことを特徴とする認証方式。

川崎人代理人 弁護士 鈴 江 武 彦